

What is claimed:

1 1. A method of improving security processing in a computing network, comprising steps of:
2 providing security processing in an operating system kernel;
3 providing an application program which makes use of the operating system kernel during
4 execution;
5 executing the application program; and
6 selectably securing at least one communication of the executing application program using
7 the provided security processing in the operating system kernel.

1 2. The method according to Claim 1, further comprising the step of:
2 configuring one or more ports used by the provided application program such that
3 communications using the configured ports are to be secured; and
4 wherein the selectably securing step then secures all communications using the configured
5 ports.

1 3. The method according to Claim 2, wherein the provided application program does not
2 include code for security processing.

1 4. The method according to Claim 2, wherein the configuring step further comprises
2 specifying information to be used by the selectably securing step.

1 5. The method according to Claim 4, wherein the specified information comprises one or

2 more of: authentication information; cipher suites options; and security key input information.

1 6. The method according to Claim 2, wherein the configuring step comprises one or more of:
2 providing port definition statements; setting environment variables; and using job control
3 language.

1 7. The method according to Claim 1, further comprising the step of providing, in the secure
2 processing, support for one or more security directives.

1 8. The method according to Claim 7, further comprising the step of invoking, during
2 execution of the provided application program, one or more of the provided security directives.

1 9. The method according to Claim 7, wherein the provided security directives comprise one
2 or more of: access capability for a client certificate; access capability for a client identifier; a
3 request to start operation of the selectably securing step; and a request to stop operation of the
4 selectably securing step.

1 10. The method according to Claim 8, wherein the provided security directives include an
2 access capability for a client certificate, and wherein the invoking step invokes the access
3 capability, and further comprising the step of returning the client certification from the provided
4 security processing to the executing application program in response to the invocation.

1 11. The method according to Claim 8, wherein the provided security directives include an
2 access capability for a client identification, and wherein the invoking step invokes the access
3 capability, and further comprising the step of returning the client identification from the provided
4 security processing to the executing application program in response to the invocation.

1 12. The method according to Claim 1, further comprising the steps of:
2 providing, in the secure processing, support for a security directive that requests the
3 selectably securing step to begin operating; and
4 invoking the security directive; and
5 wherein the selectably securing step then secures all communications of the executing
6 application program.

1 13. The method according to Claim 1, further comprising the steps of:
2 providing, in the secure processing, support for a security directive that requests the
3 selectably securing step to stop operating; and
4 invoking the security directive; and
5 wherein the selectably securing step then stops securing communications of the executing
6 application program.

1 14. The method according to Claim 12, wherein the security directive specifies information to
2 be used by the selectably securing step.

1 15. The method according to Claim 14, wherein the specified information comprises one or
2 more of: authentication information; cipher suites options; and security key input information.

1 16. The method according to Claim 12, wherein a decision to invoke the security directive is
2 made by the executing application program.

1 17. The method according to Claim 12, wherein a decision to invoke the security directive is
2 made by carrying out, by the executing application program, a security negotiation protocol.

1 18. The method according to Claim 1, wherein the provided application program includes calls
2 that invoke security processing, and further comprising steps of:
3 intercepting, in the provided security processing, the calls; and
4 executing, responsive to the interception, corresponding security functions.

1 19. The method according to Claim 1, wherein the provided application program includes calls
2 that invoke security processing, and further comprising step of interpreting, in the provided
3 security processing, the calls as being non-operative.

1 20. The method according to Claim 18, wherein the provided application program may be
2 executed on a system which does not include the provided security processing in the operating
3 system kernel, in which case the calls operate to perform security processing instead of the
4 selectably securing step.

1 21. The method according to Claim 1, wherein the provided security processing operates in a
2 Transmission Control Protocol layer of the operating system kernel.

1 22. The method according to Claim 1, wherein the provided security processing implements
2 Secure Sockets Layer.

1 23. The method according to Claim 1, wherein the provided security processing implements
2 Transaction Layer Security.

1 24. A system for improving security processing in a computing network, comprising:
2 means for performing security processing in an operating system kernel;
3 means for executing an application program which makes use of the operating system
4 kernel during execution; and
5 means for selectably securing at least one communication of the executing application
6 program using the means for performing security processing, in a manner which is transparent to
7 the executing application program.

1 25. A system for improving security processing in a computing network, comprising:
2 means for performing security processing in an operating system kernel;
3 means for executing an application program which makes use of the operating system
4 kernel during execution; and

means for selectably securing at least one communication of the executing application program using the security processing performed in the operating system kernel.

26. A computer program product for improving security processing in a computing network, the computer program product embodied on one or more computer-readable media and comprising:

computer-readable program code means for performing security processing in an operating system kernel;

computer-readable program code means for executing an application program which makes use of the operating system kernel during execution; and

computer-readable program code means for selectably securing at least one communication of the executing application program using the security processing performed in the operating system kernel.